U. S. Secret Service

Electronic Crimes Task Force Bulletin

Sharing News Among Our Law Enforcement and Industry Partners

July 2019

CURRENT TRENDS

2019 Verizon Data Breach Investigations Report Overview

On May 8, 2019, Verizon released the 2019 edition of their annual Data Breach Investigations Report (DBIR). This is the 12th edition of the DBIR and the Secret Service is proud to be a primary partner in this study.

- The Verizon DBIR is the leading industry report on trends related to data breaches and network intrusions, and is generally considered a "must-read" in the cybersecurity community.
- The 2019 Verizon DBIR includes the contributions from approximately 70 organizations from 65 countries and data on over 40,000 real-world cyber incidents from 2,013 confirmed data breaches of all types. It builds on 12 years of historical data analyzing well over 350,000 security incidents.
- The Secret Service was the first and original partner to join Verizon in compiling data and completing this annual report, contributing to every DBIR since 2010.
- The Secret Service's Criminal Investigative Division (CID) leads engagement with Verizon on the DBIR. This year, Deputy Assistant Director, Michael D'Ambrosio, contributed an article to the report entitled, "Transnational Hacker Debriefs: Insights Into Their Target Selection and Tactics, Techniques, and Procedures." (The article is located in *Appendix A* on page 65 of the report.)
- Sharing cybersecurity information continues to be an important investigative priority for the Secret Service, and the agency has long been a leader in sharing critical cybersecurity information while protecting ongoing investigations, sensitive law enforcement sources and methods, and victim privacy.

Highlights from the 2019 Verizon DBIR

- Criminal Motivations - As in prior years, the majority of malicious cyber incidents tracked in 2019 were financially motivated. The analysis shows that 71% of breaches were motivated by financial profit. This is compared to 25% of incidents that were motivated by national interest or espionage.
- Criminal Methods - Cybercriminals are still successfully using the same tried and true techniques to breach networks and commit computer-related crimes. These includes Phishing, Spear Phishing, and infected email links. Among other trends:
    - *Ransomware* - 28% of breaches involved ransomware. Ransomware is considered low risk for attackers, who do not need to be highly skilled to facilitate this type of attack.
    - *DDOS Attacks* - Distributed denial of Service (DDOS) attacks are still occurring in large numbers. Of the victims, 84% were in Finance and Insurance, 10% in Information, and 5% in Professional, Scientific, and Technical Services.

  - ➢ *ATM and Gas Pump Skimming* - Physical tampering of ATMs and gas pumps has decreased from last year. Verizon suggests this may be attributable to EMV and disruption of card-present fraud capabilities.
  - ➢ *Business Email Compromises (BECs)* - While BEC attacks remain a continuing threat, half of all US-based compromises had 99% of the money recovered or frozen; only 9% had nothing recovered.
  - ➢ *Phishing* - This year's report shows some progress on defending against phishing attacks. In exercise settings, study participants clicked on fewer than 3% of phishing attempts, down from nearly 25% in 2012. This demonstrates the value of educating computer users. However, the same research points to users being significantly more susceptible to social engineering attacks they receive on mobile devices.
- <u>Who's Responsible?</u>
  - ➢ *Outsiders* - 69% of cyberattacks were perpetrated by outsiders. This includes organized criminal groups that operate transnationally.
  - ➢ *Insiders* - 34% of the attacks were perpetrated by insiders, individuals or groups within an organization. This is particularly challenging to guard against.
- <u>Victim Error</u> - Victims continue to make the same types of mistakes that create system vulnerabilities for the cyber-criminal to exploit. These include failure to update and patch systems, to recognize malicious links and attachments, and to use encryption or multifactor authentication security features on their devices or services.
- <u>Difficulty with Detection</u>
  - ➢ This year's report again identifies a large "defender-detection deficit." Attackers are usually able to compromise an organization within minutes, while it takes organizations months to detect a compromise.
  - ➢ 40% of breaches took months to discover. In many instances, the victim does not discover the breach on their own but is instead notified by a third party such as law enforcement.

Protecting Your Organization

Protecting your data and the security of your networks comes down to your defense posture and your response plan. The stronger your defense posture and response mitigation plan the more likely the cyber attacker will opt for an easier target instead of you.

Best Practices:

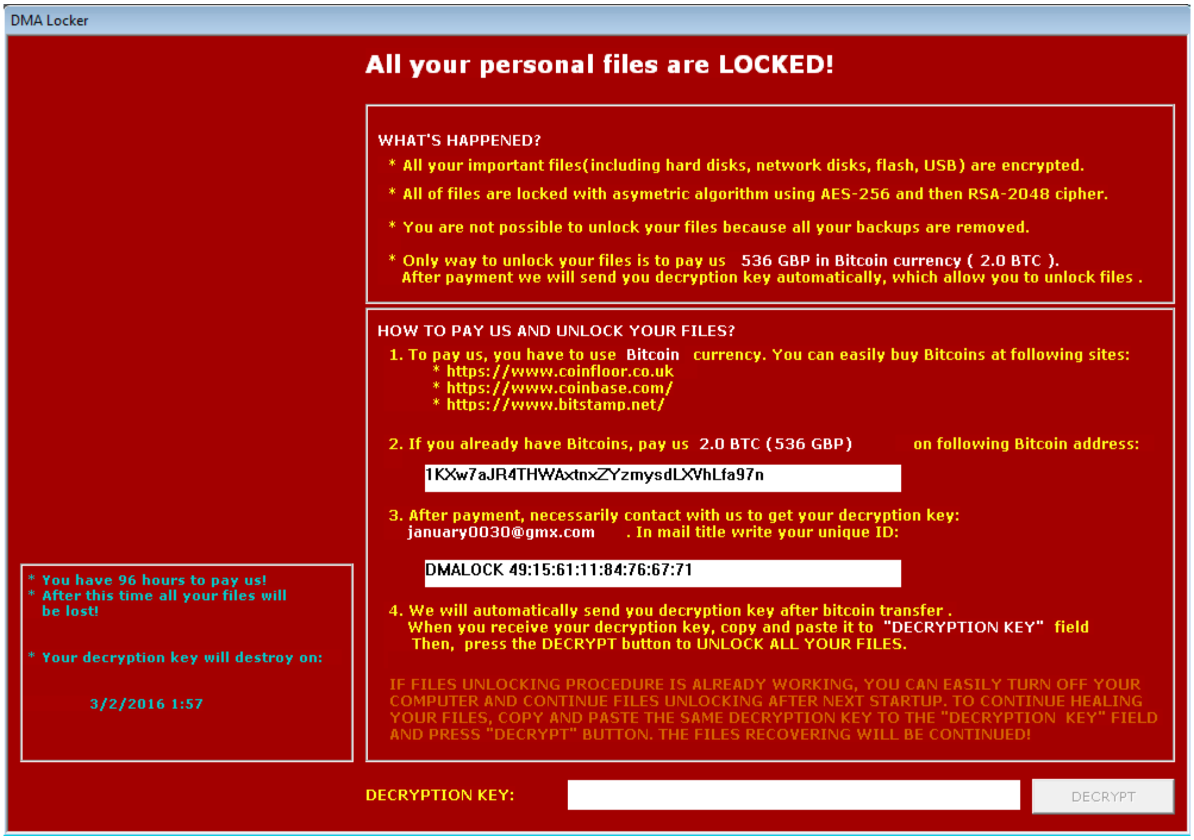
- Maintain network vigilance. Be aware of network performance and changes.
- Make your employees the first line of defense. Education and training are key.
- Principle of "least privilege." Not everyone in your organization needs network administrative privileges.
- Patch and update systems promptly.
- Encrypt sensitive data.
- Use multi-factor identification.
- Back up your data and maintain off-line.

- Have a plan for a law enforcement response in your data breach mitigation plan. Do you know who you would call when it happens?
- Ensure your physical security protocols are reviewed regularly to help safeguard against any unauthorized physical access to parts of your network.

The full 2019 DBIR is available at: https://enterprise.verizon.com/resources/reports/dbir/

Ransomware: Prevention and Response to an Attack

The USSS has recently observed and increase in notifications concerning ransomware events. Ransomware is a type of malicious software cyber actors use to deny access to systems or data. In these events, a malicious cyber actor holds systems or data hostage until a ransom is paid. Frequently, after the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If ransom demands aren't met, the system or encrypted data remains unavailable or data may be erased. This type of malware attempts to extort money from victims by displaying an on-screen alert advising the victim that their computer has been locked or that their files have been encrypted (typically using RSA 2048 encryption) and demand that a ransom is paid to restore access. The system remains encrypted until the victim pays the ransom, in exchange for a decryption key, which allows the user to regain access. Recent statistics show the average ransom demand is $522. However, this amount can be substantially higher if the target is a business or organization and not an individual. Increasingly, the ransom is demanded via virtual currency, such as payment to a Bitcoin address.



All your personal files are LOCKED!

WHAT'S HAPPENED?
* All your important files(including hard disks, network disks, flash, USB) are encrypted.
* All of files are locked with asymetric algorithm using AES-256 and then RSA-2048 cipher.
* You are not possible to unlock your files because all your backups are removed.
* Only way to unlock your files is to pay us 536 GBP in Bitcoin currency (2.0 BTC).
After payment we will send you decryption key automatically, which allow you to unlock files .

HOW TO PAY US AND UNLOCK YOUR FILES?
1. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
* https://www.coinfloor.co.uk
* https://www.coinbase.com/
* https://www.bitstamp.net/

2. If you already have Bitcoins, pay us 2.0 BTC (536 GBP) on following Bitcoin address:
1KXw7aJR4THWAxtnxZYzmysdLXVhLfa97n

3. After payment, necessarily contact with us to get your decryption key:
january0030@gmx.com . In mail title write your unique ID:
DMALOCK 49:15:61:11:84:76:67:71

4. We will automatically send you decryption key after bitcoin transfer .
When you receive your decryption key, copy and paste it to "DECRYPTION KEY" field
Then, press the DECRYPT button to UNLOCK ALL YOUR FILES.

IF FILES UNLOCKING PROCEDURE IS ALREADY WORKING, YOU CAN EASILY TURN OFF YOUR COMPUTER AND CONTINUE FILES UNLOCKING AFTER NEXT STARTUP. TO CONTINUE HEALING YOUR FILES, COPY AND PASTE THE SAME DECRYPTION KEY TO THE "DECRYPTION KEY" FIELD AND PRESS "DECRYPT" BUTTON. THE FILES RECOVERING WILL BE CONTINUED!

* You have 96 hours to pay us!
* After this time all your files will be lost!

* Your decryption key will destroy on:
3/2/2016 1:57

DECRYPTION KEY:

Responding to Ransomware Attack

Victims should reach out to law enforcement ***before*** making contact with the bad actor. Once initial contact is made, this potentially starts the clock, which will reduce the allowable time to respond.

The USSS does ***not*** encourage victims to pay the demand.

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom while others have been continually extorted by new demands.
- On average, paying the ransom results in decryption of 77% of the network data.

The following are instructions and advice an investigator can provide to the victim to help mitigate this type of network attack.

- Advise the victim to isolate the compromised portion of their network as soon as possible, but ***do not power down*** or shutoff any system affected by the ransomware (this includes both wired and wireless networks).
- Determine if communication has occurred with the attacker; if yes, by whom (if the victim is a large corporation, often it will be a company's attorney).
- Collect all available log information.
- Try to discover the characteristics of the malware infection to determine the investigative response:
    - ➢ Non-encrypting ransomware locks the screen (restricts access to files but does not encrypt them).
    - ➢ Ransomware that encrypts the Master Boot Record (MBR) prevents the victims' computers from being booted up in a live environment (what most people consider a ransomware attack).
    - ➢ Leakage or "extortionware" exfiltrates data that the attackers threaten to release if ransom is not paid
    - ➢ Mobile Device Ransomware (infects cell phones through drive-by downloads or fake apps).
- Ransomware attacks are the result of poor or defective security standards; therefore, the entire system should not be trusted. Advise the victim that all communications regarding the compromise should be "out-of-band" i.e. via phone and not email.
- If the victim has multiple backups, use the oldest back-up to restore the system-the infection should be considered to be temporal.

The below list is an example of key data to collect when responding to a ransomware event. This list is not exhaustive and every situation will be unique, but it provides a starting point for most situations.

1. Detailed victim information to include organization name, sector, systems affected, technical POC, and loss amount.
2. If available, ransomware variant name.
3. Original email(s) with full headers and any attachments (if the attack was executed by phishing).

4. Copies of any executables or other files dropped onto the system after accessing malicious attachments, including splash page.
5. Any domains or IP addresses communicated with just prior to or during infection.
6. The Bitcoin address (or other requested virtual currency address) to which payment is requested, and the amount being requested.
7. Was the ransom paid? If so, the amount and the Bitcoin address to which the payment was made.
8. If available, any forensic analysis or incident response reports completed.
9. If available, any memory captures taken during execution of the malware.
10. Status of the infection.

This information and other relevant reports related to a ransomware attack can be sent to the USSS GIOC at gioc@usss.dhs.gov, to be collected for criminal intelligence purposes. Additionally, the victim can file an Internet Crime Complaint Center (IC3) complaint at: www.ic3.gov/complaint/

Preventing a Ransomware Attack

The following measures can make a system or network more secure against malware or similar types of attacks:

- Update software and operating systems with the latest patches. This one of the most common vulnerabilities that is easily fixable.
- Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application whitelisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

DIGITAL SUCCESS STORIES

NATIONAL COMPUTER FORENSICS INSTITUTE
NATIONAL COMPUTER FORENSICS INSTITUTE
THE ELITE.
THE WORTHY.

National Computer Forensics Institute

- At the conclusion of the third quarter of FY 2019, NCFI has conducted 50 courses of instruction and trained 1,153 state and local law enforcement personnel, prosecutors and judicial officials.
- Currently in FY 2019, state and local personnel who participate in the U.S. Secret Service Forensic Partner Reporting program conducted more than 39,000 digital forensic exams in all type of criminal investigations.
- In June 2019, the NCFI hosted personnel from LexisNexis, who in partnership with the National Center for Missing and Exploited Children (NCMEC) established the Automated Delivery of Alerts on Missing Children (ADAM) Project. The program distributes missing child posters to police, companies and organizations within a specific geographic search area to fax, email and mobile devices. The NCFI has incorporated, as a part of student orientation, a briefing on the ADAM Project and NCMEC resources available to law enforcement.
- Beginning October 7, 2019, the NCFI debuts the new *Digital Evidence for Investigators* (DEI) course, which replaces the Basic Investigation of Computer and Electronic Crimes Program (BICEP) and Basic Mobil Device Investigations (BMDI) training classes at the NCFI. DEI is a 5-day course, which provides first responders/investigators a working knowledge in the identification, extrapolation and analysis of digital evidence obtained from computers and other electronic devices: cellphones, GPS units, and tablets; as well as hands-on training with forensic analysis tools, legal issues, and report generation techniques.

  NOTE: Personnel who previously completed BICEP or BMDI at the NCFI are still eligible to attend the new DEI course.

CYBER OUTREACH

The USSS National Seminar for Cyber Incident Response

The Secret Service's Criminal Investigative Division, in cooperation with the Atlanta Field Office, kicked off the inaugural National Seminar for Cyber Incident Response. This two-day event, held at LexisNexis Risk Solutions in Alpharetta, Ga., was a collaboration between the Secret Service's Electronic Crimes Task Forces and public and private sector partners.

"The National Seminar for Cyber Incident Response enhances the Secret Service's investigative mission to secure our nation's cyber related financial infrastructure," said U.S. Secret Service Director James Murray. "The collaboration between our Electronic Crimes Task Forces and our public and private partners demonstrates the commitment to combating cyber-enabled financial crimes and ensuring those responsible are held accountable."

This event featured guest speakers from across law enforcement and industry discussed: information and collaboration gaps that existed in cybersecurity; the complex cyber-threat environment; the needs and capabilities of organizations victimized by cybercrime; and investigative processes and tools of the Secret Service.

A uniquely designed cybercrime simulation exercise, facilitated by the McChrystal Group, engaged participants during a network intrusion to identify decision-making frameworks, concerns, and area for partnership between law enforcement and the private sector. “With a greater understanding of the needs of the private industry and the capabilities, investigative processes, and tools of the Secret Service, our nation can increasingly meet the challenge posed by criminal actors operating in cyberspace,” said U.S. Secret Service Atlanta Field Office Special Agent in Charge Kimberly Cheatle.

The two-day event included the following speakers:

- James Murray, Director, United States Secret Service (pictured above)
- Tom Kellerman, Chief Cyber Security Officer for Carbon Black Inc. who discussed “The American Cyber-Insurgency.”
- Jamil Farshchi, CISO Equifax, provided “Insights from a Post-Breach CISO.”
- Cyber Assistant United States Attorneys from the Northern District of Georgia presented “A view from the Prosecutors: Myths, Mitigation and More.”
- Aurobindo Sundaram, Head of Information Assurance & Data Protection at RELX spoke about “Lessons from the trenches- How to Succeed at Incident Response.”
- Author Micah Zenko gave the keynote address “Red Team Thinking and Crisis Simulations.”
- Kevin Graber, of the United States Secret Service, discussed “Enterprise Security Challenges.”

The next National Seminar for Incident Response is tentatively scheduled for November 2019 in New York, NY. Additional information on the next seminar will be provided in the near future.

Upcoming E-Skimming Briefings – The Facts and How to Protect Against It

E-Skimming has become a significant threat to U.S. businesses and the financial sector. E-Skimming is the sophisticated fraud technique where cyber criminals introduce malicious code on e-commerce payment card processing web pages to capture payment card and personally identifiable information and send the stolen data to a domain under their control. These types of attacks were first identified targeting online shopping platforms in 2000; however, since 2015 they have intensified exponentially in both scope and scale. Countless e-commerce merchants, identified and unidentified from all over the globe, have fallen victim to this hacking scheme accounting for hundreds of millions of dollars in potential and actual global monetary loss.

Due to the significant uptick of e-Skimming and its threat to all sectors who conduct e-commerce, the United States Secret Service (USSS), the Federal Bureau of Investigation (FBI) and the Department of Homeland Security’s Critical Infrastructure Security Agency (DHS-CISA) are working together to provide up-to-date e-Skimming intelligence to private industry. Held at the unclassified level, these briefings will target C-Suite level executives from a variety of organizations across the nation. The objective is to provide an overview of e-Skimming, information sharing mechanisms, and mitigation strategies.

Below is a list of locations for upcoming e-Skimming briefings and known dates. Please contact your nearest ECTF for updated briefing dates or additional information regarding their scheduled event. A list of ECTF contact numbers is listed at the back of this bulletin.

ECTF Locations	Date			
Atlanta, GA	October TBD			
Baltimore, MD	TBD			
Birmingham, AL	June 26th	*also in*	Jackson, MS	TBD
Boston, MA	TBD			
Buffalo/Syracuse, NY	August 13th			
Charlotte, NC	August 28th			
Chicago, IL	August 28th			
Cincinnati/Dayton, OH	July 17th			
Cleveland, OH	TBD			
Columbia, SC	TBD			
Dallas, TX	August TBD			
Denver, CO	August TBD			
Detroit, MI	July 31st			
Honolulu, HI	August TBD			
Houston, TX	August 21st			
Kansas City, MO	August 26th			
Las Vegas, NV	August 28th	*also in*	Reno/Tahoe, NV	July 17th
Los Angeles, CA	August 28th			
Louisville, KY	October TBD			
Memphis, TN	August TBD			
Miami, FL	August 22nd			
Minneapolis, MN	September 16th			
Nashville, TN	September TBD			
Newark, NJ	August 13th (in New York City)			
New Orleans, LA	TBD			
New York, NY	August 13th			
Oklahoma City, OK	July 10th & September 6th			
Orlando, FL	TBD			
Philadelphia, PA	August TBD			
Phoenix, AZ	August 22nd			
Pittsburgh, PA	TBD			
San Antonio, TX	June 28th			
San Diego, CA	August 6th			
San Francisco, CA	August 29th			
Seattle, WA	September 5th			
St. Louis, MO	September 5th			
Tampa, FL	August 19th			
Washington, DC	August TBD			
London, England	TBD			

LEGAL AND POLICY DEVELOPMENTS

Introducing the U.S. Secret Service *Cyber Investigations Advisory Board (CIAB)*

On May 26, 2019, Department of Homeland Security (DHS) Acting Secretary Kevin McAleenan approved the formation of the U.S. Secret Service *Cyber Investigations Advisory Board (CIAB)*, a new Federal Advisory Committee. The goal of CIAB is to provide Secret Service's Office of Investigations with outside strategic input for the agency's investigative mission, including insights on the latest trends in cybercrime, financial crime, technology and investigative techniques. The CIAB will serve as a key mechanism through which senior industry and academic experts can engage, collaborate, and provide guidance to the Secret Service regarding cybersecurity and cybercrime issues. It is anticipated that much of the information and advice provided by the CIAB will be made available to the ECTFs.

About the CIAB: The CIAB will consist of up to 16 members comprised industry executives and academic experts. Board membership will represent a diverse range of industries and sectors including banking, finance, and communications. Further, in order to provide institutional context for those board members who may not be closely familiar with the Secret Service investigative mission, membership will also include several retired Secret Service Special Agents. Members appointed to the board will serve a term of two years, with opportunities to renew for up to three terms. The aim is to announce the CIAB board members by the Fall of 2019 and to hold the first board meeting in the Winter of 2020. Meetings will be held semiannually thereafter.

Recent Legislative Changes to 18 USC 3056

A small change by Congress to our authorizing statute could pay big dividends to the U.S. Secret Service's state and local law enforcement partners—particularly those who participate in the Electronic Crimes Task Forces. The Trafficking Victims Protection Act of 2017 amended 18 U.S.C. 3056 to specifically allow the Secret Service to provide forensic and investigative assistance to state or local law enforcement.

Prior to December 21, 2018, when the Trafficking Victims Protection Act was enacted, the Secret Service had been specifically authorized only to provide assistance to state and locals law enforcement in support of an investigation involving a missing or exploited child. By broadening the Secret Service's authority to provide forensic and investigative assistance to state and locals, Congress is recognizing the expertise that the ECTFs provide. Indeed, a specific mandate to help state and locals will permit investigators to leverage their skills in order to solve a wider array of crimes.

CURRENT ECTF LOCATIONS

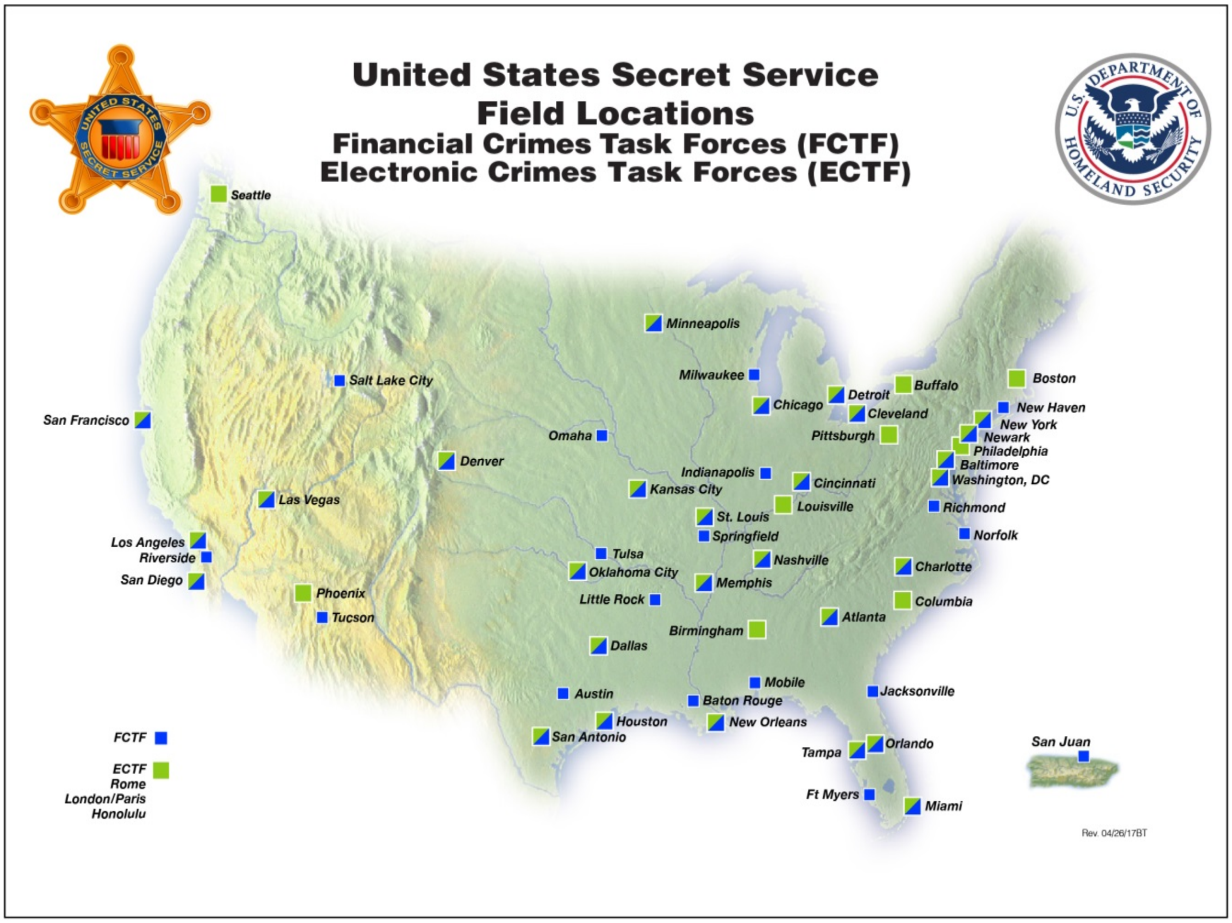
Atlanta, GA
404-331-6111
Baltimore, MD
443-263-1100
Birmingham, AL
205-731-1144
Boston, MA
617-565-5640
Buffalo, NY
716-551-4401
Charlotte, NC
704-442-8370
Chicago, IL
312-353-5431
Cincinnati, OH
513-684-3585
Cleveland, OH
216-750-2058
Columbia, SC
803-772-4015

Dallas, TX
972-868-3200
Denver, CO
303-850-2700
Detroit, MI
313-226-6400
Honolulu, HI
808-541-1912
Houston, TX
713-868-2299
Kansas City, MO
816-460-0600
Las Vegas, NV
702-868-3000
Los Angeles, CA
213-894-4830
Louisville, KY
502-582-5171
Memphis, TN
901-544-0333

Miami, FL
305-863-5000
Minneapolis, MN
612-348-1800
Nashville, TN
615-736-5841
Newark, NJ
973-971-3100
New Orleans, LA
504-841-3260
New York, NY
718-840-1000
Oklahoma City, OK
405-272-0630
Orlando, FL
407-648-6333
Philadelphia, PA
215-861-3300
Phoenix, AZ
602-640-5580

Pittsburgh, PA
412-281-7825
San Antonio, TX
210-308-6220
San Diego, CA
619-557-5640
San Francisco, CA
415-576-1210
Seattle, WA
206-553-1922
St. Louis, MO
314-539-2238
Tampa, FL
813-228-2636
Washington, DC
202-406-8000

London, England
Rome, Italy


United States Secret Service
Field Locations
Financial Crimes Task Forces (FCTF)
Electronic Crimes Task Forces (ECTF)
UNITED STATES SECRET SERVICE
U.S. DEPARTMENT OF HOMELAND SECURITY
Seattle
Minneapolis
Salt Lake City
Milwaukee
Boston
Buffalo
Detroit
Chicago
Cleveland
New Haven
New York
Newark
Philadelphia
Baltimore
Washington, DC
Pittsburgh
San Francisco
Omaha
Denver
Indianapolis
Kansas City
Cincinnati
Louisville
Las Vegas
St. Louis
Springfield
Richmond
Norfolk
Los Angeles
Riverside
San Diego
Tulsa
Oklahoma City
Nashville
Charlotte
Memphis
Phoenix
Tucson
Little Rock
Columbia
Atlanta
Birmingham
Dallas
Mobile
Jacksonville
Austin
Baton Rouge
Houston
New Orleans
San Antonio
Orlando
Tampa
San Juan
Ft Myers
Miami
FCTF ■
ECTF ■
Rome
London/Paris
Honolulu
Rev. 04/26/17BT